J. Symbolic Computation (1992) **13**, 463-472

PRODUCTS OF POLYNOMIALS AND A PRIORI ESTIMATES FOR COEFFICIENTS IN POLYNOMIAL DECOMPOSITIONS : A SHARP RESULT.

BERNARD BEAUZAMY

Institut de Calcul Mathématique, Université de Paris 7, 2 Place Jussieu, 75251 Paris Cedex 05 - France.

Received 22 November 1990

Using a result of E. Bombieri which appeared in Beauzamy, Bombieri, Enflo and Montgomery (1990), we introduce a weighted norm on the space of polynomials in one variable ; the weights are much smaller than 1. For this norm, we give a precise estimate for products of polynomials : the numerical constant we obtain is best possible. The norm, moreover, is submultiplicative.

If P is a polynomial with integer coefficients, we deduce from the above result an a priori estimate for the size of the coefficients in any factor of P, which strongly improves all the existing ones.

Let $P(z) = \sum_{j=0}^{d} a_j z^j$ be a polynomial with one complex variable and integer coefficients ($a_j \in \mathbb{Z}$). If P is factored as $P = Q \cdot R$, where Q and R themselves are in $\mathbb{Z}[z]$, what is the maximum of modulus of the coefficients in Q and R ? Can it be predicted before the decomposition is written ? Before answering this question, let's explain its origin.

1. The factorization algorithm

The above problem has received considerable attention, since the existence of such an priori bound is an essential feature for the design of efficient factorization

0747-7171/92/050463+10 $03.00/0 © 1992 Academic Press Limited

algorithms in symbolic computation (H. Zassenhaus (1969), P. Wang and B. M. Trager (1979), P. Wang (1983)).

Indeed, suppose we want to factor P in $\mathbb{Z}[z]$. We can assume that P is primitive (that is : no factor divides all coefficients in P) and that P and its derivative P' are relatively prime.

We choose a prime q, not dividing the leading coefficient of P. Let P_0 be the image of P in $\mathbb{Z}_q[z]$. The prime q has also to be chosen so that P_0 has no multiple zero in $\mathbb{Z}_q[z]$.

Then P_0 is factored in $\mathbb{Z}_q[z]$. This is fast, since all coefficients of P_0 are smaller than q. Let $P_0 = Q_0 \cdot R_0$ be the factorization in $\mathbb{Z}_q[z]$ (we write only two factors for simplicity). Then

$$P \equiv P_0 = Q_0 \cdot R_0 , \qquad (\text{mod } q).$$

Using Hensel's Lemma (H. Zassenhaus (1969)), we can lift the factors modulo q into a decomposition modulo q^2. Precisely, we find Q_1, R_1 in $\mathbb{Z}_{q^2}[z]$ such that :

$$Q_1 \equiv Q_0 \quad (\text{mod } q) \quad , \quad R_1 \equiv R_0 \quad (\text{mod } q),$$

and if $P_1 = Q_1 \cdot R_1$, then $P \equiv P_1 \pmod{q^2}$.

Let B be the bound we are looking for, namely the maximum (in modulus) of all coefficients in any factor of P. We repeat the lifting procedure with q^2, q^4, ..., q^{2^k}, until $q^{2^k} \geq 2B$, so we find $Q_2, Q_3, \ldots, Q_k, R_2, R_3, \ldots R_k$, with

$$Q_j \equiv Q_{j-1} \quad (\text{mod } q^{2^{j-1}}) \quad , \quad R_j \equiv R_{j-1} \quad (\text{mod } q^{2^{j-1}}),$$

and

$$P \equiv Q_k \cdot R_k \quad (\text{mod } q^{2^k}).$$

We stop the lifting process at this point, and the algorithm now becomes a trial process : in $\mathbb{Z}[z]$, we try to divide P by Q_k, R_k, ..., or by combinations of these factors. If P has true factors, they will appear this way. However, it may happen that P is irreducible, though each factor in $\mathbb{Z}_{q^j}[z]$ was non-trivial.

The existence of the a priori bound B is therefore essential to determine the stopping time for the lifting process. Since this process is costly, the bound should be as small as possible.

The first estimates were given by H. Zassenhaus (1969). Later, M. Mignotte observed (1974) that the problem was connected to estimates for products of polynomials, and made use of Mahler's measure :

$$M(P) = \exp \int_0^{2\pi} \log |P(e^{i\theta})| \frac{d\theta}{2\pi} .$$

When no information at all is known on the degree of Q, this led to the estimate

$$|Q|_1 \leq 2^d M(P), \tag{1.1}$$

where d is the degree of P and

$$|Q|_1 = \sum_{j=0}^{m} |b_j| , \text{ if } Q(z) = \sum_{j=0}^{m} b_j z^j .$$

Since $M(P)$ is not easy to compute in practice (see Cierlenco, Mignotte, Piras (1987) for an approach), the estimate (1.1) is usually replaced by the weaker, but more convenient one :

$$|Q|_1 \leq 2^d |P|_2 , \tag{1.2}$$

with

$$|P|_2 = (\sum |a_j|^2)^{1/2} .$$

and each coefficient b_j in Q satisfies

$$|b_j| \leq \binom{m}{j} |P|_2 , \tag{1.3}$$

where, as before, m is the degree of Q. This implies

$$\max |b_j| \leq \binom{m}{[m/2]} |P|_2 \leq \binom{d}{[d/2]} |P|_2 . \tag{1.4}$$

Estimate (1.3) was improved by Mignotte (1988) in some special cases, for instance when $M(P)$ is not too large.

2. The results

We prove here an a priori estimate sharper than (1.1), valid with no restriction. We make no use of Mahler's measure, but instead we use the definitions of Beauzamy, Bombieri, Enflo and Montgomery (1990) and Bombieri's results in this paper. First, we define a new norm.

Let $P = \sum_0^d a_j z^j$ be a polynomial and d its degree. We define :

$$[P]_2 = \left(\sum_0^d \frac{1}{\binom{d}{j}} |a_j|^2 \right)^{1/2} . \tag{2.1}$$

which is a weighted l_2 norm, satifying

$$[P]_2 \leq |P|_2 .$$

It should be observed that the norm depends on the degree, but this dependence is omitted in the notation. We have :

Theorem 1. – *Let Q, R be polynomials in one variable, of degrees m and n respectively. Then :*

$$[QR]_2 \geq \sqrt{\frac{m!n!}{(m+n)!}} [Q]_2 [R]_2 ; \tag{2.2}$$

this result is best possible.

We will apply this result to get an upper bound on the size of coefficients in Q or R, knowing the size of the coefficients in the product $P = Q \cdot R$. We can of course assume that P does not vanish at 0. We obtain :

Theorem 2. – *Let P in $\mathbb{Z}[z]$, with $P(0) \neq 0$, and let $P = Q \cdot R$ be any factorization in $\mathbb{Z}[z]$. Then any coefficient b_j in Q satisfies :*

$$|b_j| \leq \sqrt{\frac{1}{2}\binom{m}{j}\binom{d}{m}} [P]_2 = \sqrt{\frac{d!}{2(d-m)!(m-j)!j!}} [P]_2. \tag{2.3}$$

From this result, we deduce the main theorem of the present paper :

Theorem 3. – *Let P in $\mathbb{Z}[z]$, with $P(0) \neq 0$, and let Q be any factor of P in $\mathbb{Z}[z]$. Then the coefficients b_j in Q satisfy :*

$$\max_j |b_j| \leq \frac{3^{3/4}}{2\sqrt{\pi}} \frac{3^{d/2}}{\sqrt{d}} [P]_2 . \tag{2.4}$$

The estimate (2.4) is obviously better than (1.4), for two reasons. First, $3^{d/2}/\sqrt{d} < \binom{d}{[d/2]}$, and second (and main reason), the norm $[P]_2$ is smaller (and usually *much smaller*) than the usual l_2-norm.

We now turn to the proofs.

Proof of Theorem 1. – We use a result of Bombieri in Beauzamy et al., (1990), concerning polynomials in many variables. We recall that, if

$$\tilde{Q}(z_1, \ldots, z_N) = \sum_\beta b_\beta z_1^{\beta_1} \ldots z_N^{\beta_N} , \quad \tilde{R}(z_1, \ldots, z_N) = \sum_\gamma c_\gamma z_1^{\gamma_1} \ldots z_N^{\gamma_N} ,$$

are homogeneous polynomials in N variables, with complex coefficients, of degrees m and n respectively, and if we define :

$$[\tilde{Q}]_2 = \Big(\sum_{|\beta|=m} \frac{\beta!}{m!} |b_\beta|^2 \Big)^{1/2} ,$$

with $\beta! = \beta_1! \cdots \beta_N!$, $|\beta| = \beta_1 + \cdots + \beta_N$, we have

$$[\tilde{Q}\tilde{R}]_2 \geq \sqrt{\frac{m!n!}{(m+n)!}} [\tilde{Q}]_2 [\tilde{R}]_2 , \tag{2.5}$$

Now if $P(z) = \sum_0^d a_j z^j$ is a polynomial in one variable, we define

$$\tilde{P}(z, z') = \sum_{j=0}^{d} a_j z^j z'^{m-j} ,$$

which is a homogeneous polynomial of degree d, in two variables. One checks immediately that

$$[P]_2 = [\tilde{P}]_2 .$$

Let $P = Q \cdot R$ be any factorization of P. One checks also that $\widetilde{QR} = \tilde{Q}\tilde{R}$, and Theorem 1 is proved.

In Beauzamy et al. (1990), it has been proved that the constant given in (2.2) is best possible, but among all constants *independent of the number of variables.* This does not imply that it is best possible in our case, and we have to check this directly. Consider $Q = 2^{-n/2}(1-z)^n$, so $[Q]_2 = 1$, $R = 2^{-n/2}(1+z)^n$, so $[R]_2 = 1$, and

$$[QR]_2 = 2^{-n} \left(\sum_0^n \frac{\binom{n}{j}^2}{\binom{2n}{2j}} \right)^{1/2} .$$

We will show that this last quantity is equal to $\sqrt{n!^2/(2n)!}$. This assertion is equivalent to

$$2^{-2n} \sum_0^n \frac{\binom{n}{j}^2}{\binom{2n}{2j}} = 1/\binom{2n}{n} ,$$

or

$$\sum_0^n \frac{\binom{2n}{n}\binom{n}{j}^2}{\binom{2n}{2j}} = 4^n ,$$

which is the same as

$$\sum_0^n \frac{(2n-2j)!(2j)!}{(n-j)!^2 j!^2} = 4^n ,$$

$$\sum_0^n \binom{2n-2j}{n-j}\binom{2j}{j} = 4^n ,$$

which is formula 3.90 of Gould's book (1972).

We now turn to the proof of Theorem 2. If R has coefficients in $\mathbb{Z}$, the first and last coefficients have modulus ≥ 1. So $[R]_2 \geq \sqrt{2}$, and we find

$$\sum_{j=0}^m \frac{|b_j|^2}{\binom{m}{j}} \leq \frac{(m+n)!}{2m!n!} [P]_2^2 ,$$

and therefore, for each coefficient b_j,

$$|b_j| \leq \sqrt{\frac{1}{2}\binom{m}{j}\binom{d}{m}}\, [P]_2 , \tag{2.6}$$

as we announced. We observe that the fact that R has integer coefficients is used only at one place, and could be replaced by the assumption that all non- zero coefficients in R are in modulus larger than 1. This proves Theorem 2.

To prove Theorem 3, we observe that, for given d, m, the largest estimate in (2.3) is obtained for $j = [m/2]$. Thus we get :

$$\max_j |b_j| \leq \sqrt{\frac{d!}{2(d-m)![m/2]!^2}}\,[P]_2 , \tag{2.7}$$

an upper bound which can be useful when the degree of Q (that is m) is known. Stirling's formula, in this case, gives the upper estimate :

$$\max_j |b_j| \leq \frac{2^{\frac{m}{2}-\frac{1}{2}}\, d^{\frac{d}{2}+\frac{1}{4}}}{\pi^{\frac{1}{2}}(d-m)^{\frac{1}{2}(d-m)+\frac{1}{4}}\, m^{\frac{1}{2}m+\frac{1}{4}}}\,[P]_2 . \tag{2.8}$$

If no information is known on m, we deduce from (2.6)

$$|b_j| \leq \sqrt{\frac{d!}{2(d-m)!(m-j)!j!}}\,[P]_2 .$$

The denominator is of the form $x!y!z!$, with $x+y+z=d$. The use of Stirling's formula, followed by a minimization on x, y, z of the quantities involved, give

$$\max_j |b_j| \leq \frac{3^{3/4}}{2\sqrt{\pi}}\,\frac{3^{d/2}}{\sqrt{d}}\,[P]_2 ,$$

as we announced.

Examples. – For the polynomial $P = 2+2z^2-5z^3+6z^4+z^5+z^6$ cited in Cerlienco, Mignotte, Piras (1987), the classical estimate $2^d M(P)$ gives 448 ; Theorem 2 gives 62.8. For $P = 1-7z^2+z^4 = (1-3z+z^2)(1+3z+z^2)$, with $d=4$, $m=2$, the classical estimate (2) gives 14.28 ; our Theorem 3 gives 7.81. In fact, the bigger the central coefficients will be in P, the stronger will be the improvement brought by Theorems 2 and 3.

The interest of the estimate given by Theorem 3 comes mainly from two facts : first, the norm $[P]_2$ is explicit (unlike Mahler's measure), and can be computed immediately, using the coefficients only, and second it is usually much smaller than the usual $|\cdot|_2$ - norm : it carries weights which are much smaller than 1. Indeed, it can very well be smaller than Mahler's measure : if we take the example, cited above, of the polynomial :

$$P(z) = 2+2z^2-5z^3+6z^4+z^5+z^6 ,$$

we know from Cerlienco, Mignotte, Piras (1987) that $M(P) \sim 7.04$, whereas $[P]_2 = 3.01$.

Comparison with Mahler's measure is easy to obtain :

Proposition 4. – *If P has degree d,*

$$\binom{d}{[d/2]}^{-1/2} M(P) \leq [P]_2 \leq 2^{d/2} M(P) ,$$

and these inequalities are best possible.

Proof. – We know from Kurt Mahler (1960) that any coefficient a_j in P satisfies :

$$|a_j| \leq \binom{d}{j} M(P).$$

Summing over j gives the right-hand side inequality. The example of $(1+z)^d$ shows that the inequality is best possible. The left-hand side inequality is obvious, since $\binom{d}{[d/2]}$ is the largest of all coefficients. The fact that the inequality is best possible is seen by considering the polynomial $P = \binom{d}{[d/2]} z^{[d/2]} + z^d$, or $P = 1 + \binom{d}{[d/2]} z^{[d/2]} + z^d$.

The norm $[\cdot]_2$ has one more interesting property, namely to be *submultiplicative* :

Proposition 5. – *For any polynomials Q and R,*

$$[Q \cdot R]_2 \leq [Q]_2 \cdot [R]_2 .$$

Proof. – Let's write :

$$Q(z) = \sum_0^m b_j z^j , \quad R(z) = \sum_0^n c_{j'} z^{j'} , \quad P(z) = Q(z) \cdot R(z) = \sum_0^{m+n} a_l z^l ,$$

with $a_l = \sum_{j=0}^{l} b_j c_{l-j}$.

It's enough, of course, to show the property when all coefficients are real positive : this will simplify the notation.

In order to show that

$$\sum_0^{m+n} \frac{1}{\binom{m+n}{l}} \Big(\sum_{j=0}^{l} b_j c_{l-j} \Big)^2 \leq \sum_{j=0}^{m} \frac{b_j^2}{\binom{m}{j}} \sum_{j'=0}^{n} \frac{c_{j'}^2}{\binom{n}{j'}} ,$$

it is of course enough to show that, for all l,

$$\frac{1}{\binom{m+n}{l}}\Big(\sum_{j=0}^{l} b_j c_{l-j}\Big)^2 \leq \sum_{j=0}^{l} \frac{b_j^2}{\binom{m}{j}} \frac{c_{l-j}^2}{\binom{n}{l-j}} .$$

The Cauchy-Schwarz inequality gives :

$$\sum_l b_j c_{l-j} \leq \left(\sum_{j=0}^{l} \frac{b_j^2}{\binom{m}{j}} \frac{c_{l-j}^2}{\binom{n}{l-j}}\right)^{1/2} \left(\sum_{j=0}^{l} \binom{m}{j}\binom{n}{l-j}\right)^{1/2} .$$

But

$$\sum_{j=0}^{l} \binom{m}{j}\binom{n}{l-j} = \binom{m+n}{l} ,$$

and the result is proved.

So the norm $|\cdot|_2$ has convenient properties for practical purposes.

For homogeneous polynomials in many variables, similar results hold. The estimate (2.5) gives immediately :

Theorem 6. – *Let $\tilde{P}$ a homogeneous polynomial in many variables, with coefficients in $\mathbb{Z}$ and with (total) degree d. Let $\tilde{P} = \tilde{Q}\tilde{R}$ be any factorization in $\mathbb{Z}[z_1, \ldots z_N]$. Then, the coefficients b_β in Q satisfy :*

$$|b_\beta| \leq \sqrt{\frac{1}{2}\frac{m!}{\beta!}\binom{d}{m}}\,|\tilde{P}|_2 = \sqrt{\frac{d!}{2(d-m)!\beta!}}\,|P|_2 , \tag{2.9}$$

where m is the degree of Q.

From (2.9) follows the crude upper estimate :

$$|b_\beta| \leq \sqrt{\frac{d!}{2}}\,|\tilde{P}|_2 ,$$

which provides an a priori bound for the many-variable factorization problem. This bound is itself independent of the number of variables.

Acknowledgements

This work was supported by Contract 89/1377, Ministry of Defense, D.G.A./ D.R.E.T. – France.

Part of this paper was written while the author was Visiting Professor at Kent State University, and benefitted from its nice hospitality. Thanks are also due to Vilmar Trevisan, for several conversations about the factorization algorithms and its computer implementations, and to the Mathematics Library of the University of Illinois at Urbana-Champaign, which supplied a copy of Gould's book, unavailable in Paris.

References

Beauzamy, B., Bombieri, E., Enflo, P., Montgomery, H. (1990). Products of polynomials in many variables. Journal of Number Theory, vol. 36, 2, 219–245.

Cerlienco, L., Mignotte, M., Piras, F. (1987). Computing the measure of a polynomial. J. Symbolic Computation, 4, 21–33.

Gould, H.W. (1972). Combinatorial Identities, Morgantown.

Mahler, K. (1960). An application of Jensen's formula to polynomials. Mathematika 7, 98–100.

Mignotte, M. (1974). An Inequality About Factors of Polynomials. Mathematics of Computation, vol. 28, 128, 1153–1157.

Mignotte, M. (1988). An Inequality about Irreducible Factors of Integer Polynomials. Journal of Number Theory, vol. 30, 2, 156-166.

Wang, P. S., Trager, B. M. (1979). New algorithms for polynomial square-free decompositions over the integers. SIAM Journal of Computing, vol. 8, 3, 300-305.

Wang, P. S. (1983). Early detection of true factors in univariate polynomial factorizations. Proceedings A.C.M. EUROCAL, London, March 28-30.

Zassenhaus, H. (1969). On Hensel factorization. Journal of Number Theory, 1, 291–301.